

# HA with Multiple Databases Deployment Guide

FortiClient EMS 7.0



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



March 05, 2024

FortiClient EMS 7.0 HA with Multiple Databases Deployment Guide

04-700-793731-20240305

# TABLE OF CONTENTS

<b>Change log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
<b>SQL Server Failover Cluster Instances</b>	<b>6</b>
Configuring AD and DNS settings	8
Configuring iSCSI virtual disks	9
Configuring Windows clustering	12
Configuring Microsoft SQL database clustering	14
Configuring EMS HA	15
Upgrading EMS HA	20
Frequently asked questions	22
<b>Always on HA in multisubnet environment</b>	<b>23</b>
Configuring Active Directory and DNS settings	24
Configuring Windows clustering	25
Installing SQL and enabling always on HA	26
Installing EMS and configuring SQL always on HA	27
Installing EMS and configuring SQL always on HA (EMS 7.0.6 or older)	28
Installing EMS and configuring SQL always on HA (EMS 7.0.7 or newer)	31
Configuring EMS	35
Upgrading EMS HA	36
Managing a custom site with an availability group	38
Restoring a backup	40

# Change log

Date	Change Description
2022-04-06	Initial release.
2022-04-26	Updated <a href="#">Configuring EMS HA on page 15</a> .
2022-05-24	Added <a href="#">Always on HA in multisubnet environment on page 23</a> .
2022-06-13	Updated <a href="#">Configuring Active Directory and DNS settings on page 24</a> , <a href="#">Installing EMS and configuring SQL always on HA (EMS 7.0.6 or older) on page 28</a> , and <a href="#">Managing a custom site with an availability group on page 38</a> .
2022-06-23	Added <a href="#">Restoring a backup on page 40</a> . Updated <a href="#">Installing EMS and configuring SQL always on HA (EMS 7.0.6 or older) on page 28</a> and <a href="#">Managing a custom site with an availability group on page 38</a> .
2023-02-15	Added <a href="#">Upgrading EMS HA on page 36</a> . Updated: <ul style="list-style-type: none"><li>• <a href="#">SQL Server Failover Cluster Instances on page 6</a></li><li>• <a href="#">Configuring EMS HA on page 15</a></li><li>• <a href="#">Upgrading EMS HA on page 20</a></li><li>• <a href="#">Always on HA in multisubnet environment on page 23</a></li><li>• <a href="#">Configuring Active Directory and DNS settings on page 24</a></li><li>• <a href="#">Installing EMS and configuring SQL always on HA (EMS 7.0.6 or older) on page 28</a></li><li>• <a href="#">Installing EMS and configuring SQL always on HA (EMS 7.0.7 or newer) on page 31</a></li><li>• <a href="#">Restoring a backup on page 40</a></li></ul>
2023-04-13	Updated: <ul style="list-style-type: none"><li>• <a href="#">Always on HA in multisubnet environment on page 23</a></li><li>• <a href="#">Installing SQL and enabling always on HA on page 26</a></li><li>• <a href="#">Installing EMS and configuring SQL always on HA (EMS 7.0.7 or newer) on page 31</a></li></ul>
2023-08-04	Updated: <ul style="list-style-type: none"><li>• <a href="#">SQL Server Failover Cluster Instances on page 6</a></li><li>• <a href="#">Configuring EMS HA on page 15</a></li></ul>
2024-03-05	Updated: <ul style="list-style-type: none"><li>• <a href="#">Configuring EMS HA on page 15</a></li><li>• <a href="#">Upgrading EMS HA on page 20</a></li><li>• <a href="#">Installing EMS and configuring SQL always on HA (EMS 7.0.6 or older) on page 28</a></li><li>• <a href="#">Installing EMS and configuring SQL always on HA (EMS 7.0.7 or newer) on page 31</a></li><li>• <a href="#">Upgrading EMS HA on page 36</a></li></ul>

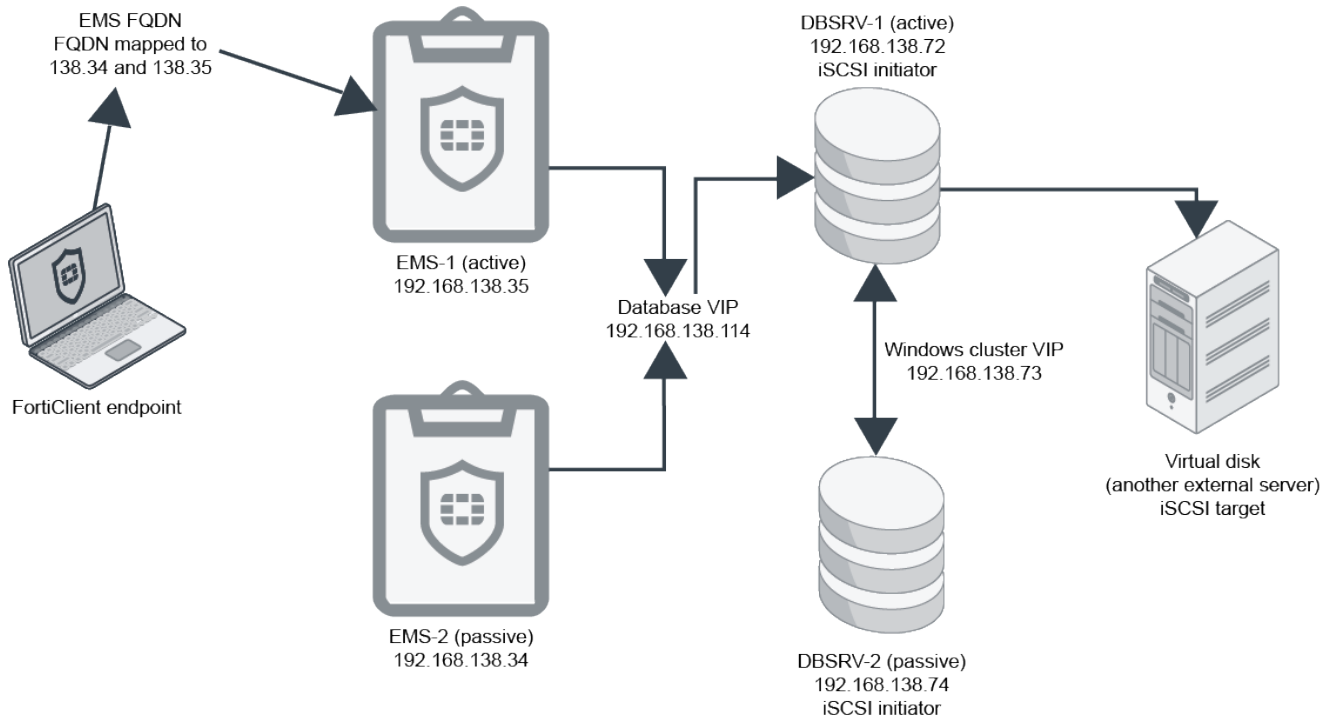
# Introduction

This guide contains deployment instructions when using high availability with FortiClient EMS. See the following deployment scenarios:

# SQL Server Failover Cluster Instances

This document provides information about deploying FortiClient EMS using high availability (HA). It aims to provide a step-by-step guide on EMS HA with some basic coverage of database clustering. There may be inaccuracies as regards to database clustering. This guide does not represent proper architecture design from a database clustering standpoint. Do not use this guide for database architecture design.

This deployment does not support SQL Server Express for SQL clustering.



The example deployment that this document describes uses the following components:

- FortiClient EMS
- FortiClient
- Windows Server 2019 Standard Edition
- Microsoft SQL Server 2017 Enterprise
- Microsoft SQL Server Management Studio 18

Note the following:

- For EMS 7.0.7 and earlier versions, you must enable FILESTREAM on the SQL Server Database Engine instance for file synchronization between HA nodes. See [Enable and configure FILESTREAM](#).
- For EMS 7.0.8 and later versions, sharing files between EMS nodes relies on network shares that different EMS nodes can access.

- There are multiple ways to implement DNS and load balancing to handle EMS failover:

Method	Description
DNS round robin or failover	EMS running in HA mode must always configure a fully qualified domain name (FQDN), and FortiClient endpoints must point to a DNS server that has enabled DNS round robin or supports DNS failover, so that endpoints can always connect to the correct primary EMS server. Endpoint users must ensure that endpoints do not cache the DNS result for more than 30 seconds so that FortiClient can resolve the FQDN to the new primary EMS server with a new IP address in case EMS failover happens quickly.
Load balancer	DNS round robin configuration may cause Fortinet Security Fabric connector to send data to the failover node, which by design has all but the monitor FCEMS services off. This results in Fabric connection failure. To overcome this limitation, set up the <a href="#">Fabric connection using traffic manager</a> or <a href="#">FortiGates as a load balancer</a> .

- If logged in to an EMS server as a domain user, add the domain user to the local logon as a service. Otherwise, EMS services may not start up properly.

## Configuring AD and DNS settings

This deployment has the following prerequisites:

- All servers and virtual machines must belong to the same domain.
- In this deployment, the Active Directory (AD) server also acts as a DNS server. The configuration requires you to configure DNS settings in AD.

### To configure AD and DNS:

1. In Server Manager on the AD Server, go to *Tools > DNS*.
2. Right-click the DNS server, then select *Properties*.
3. In the *Properties* dialog, go to the *Advanced* tab.
4. Ensure that *Enable round robin* is selected. Click *OK*.
5. Create two A records on the DNS server that have the same name, but point to their respective EMS servers. In this example, the records share the name "emsha". One points to 192.168.138.35, which is "EMS-Active". The other points to 192.168.138.34, which is "EMS-Passive".

The screenshot shows the Windows DNS Manager interface. The left-hand tree view is expanded to 'Forward Lookup Zones' under the 'WIN-NDIL9K7TGL6' server. The right-hand pane displays a list of DNS zones and records. The 'emsha' zone is selected and highlighted in blue. The table below represents the data shown in the right pane.

Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[493], win-ndil9k7tg16.ericl...	static
(same as parent folder)	Name Server (NS)	win-ndil9k7tg16.ericleong....	static
(same as parent folder)	Host (A)	192.168.138.36	11/2/2021 3:00:00 PM
DBSRV1	Host (A)	192.168.138.72	11/2/2021 3:00:00 PM
DBSRV2	Host (A)	192.168.138.74	11/2/2021 3:00:00 PM
emsdcluster	Host (A)	192.168.138.73	11/2/2021 3:00:00 PM
emsha	Host (A)	192.168.138.35	static
emsha	Host (A)	192.168.138.34	static

- On a system joined to the AD, open Command Prompt and run `nslookup <DNS record name>.<domain>`. It should return the two IP addresses of the EMS instances that you configured in step 5.

```
C:\Users\administrator.█>nslookup emsha.█.com
Server: UnKnown
Address: 192.168.138.36

Name:    emsha.█.com
Addresses: 192.168.138.34
          192.168.138.35
```



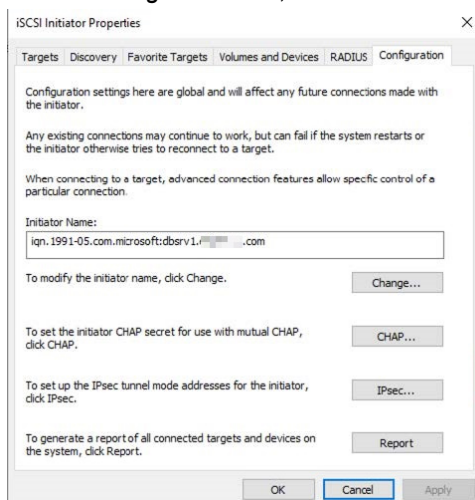
## Configuring iSCSI virtual disks

Configuring iSCSI virtual disks is required for the Windows clustering setup that this guide later describes. The iSCSI initiator is where all database read/write activity is initiated. The iSCSI target is the actual disk that the initiator writes to.

The virtual disk is critical, as database servers write into this disk. If the disk is offline, database services are disrupted, affecting EMS operations. You should engage with relevant Microsoft parties to plan a highly scalable database infrastructure. This is a Microsoft SQL requirement and is unrelated to EMS requirements.

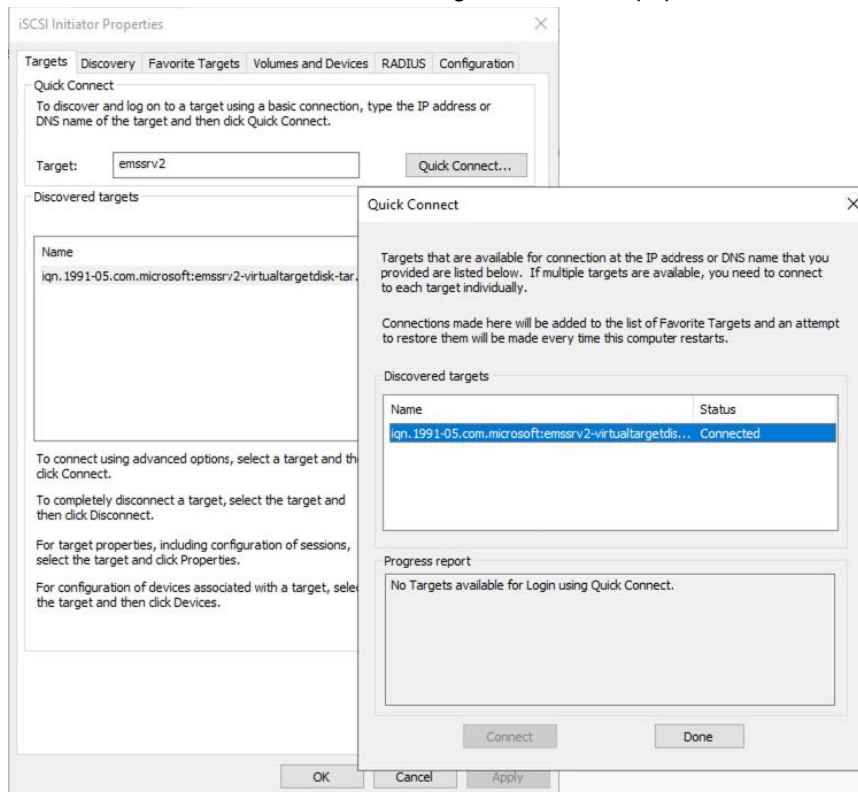
**To configure iSCSI virtual disks:**

1. Create a new volume in the iSCSI target server. In this example, the iSCSI target server is an EMS server. This is not best practice and does not provide a proper availability design from a database clustering point of view.
2. Install the iSCSI target server role:
  - a. In Server Manager, on the *Manage* menu, click *add Roles and Features*.
  - b. Proceed to the *Server Roles* page. Under *File and Storage Services* > *File and iSCSI Services*, select *iSCSI Target Server*. Click *Install*.
3. Create the virtual disk:
  - a. After the server installs the role, in Server Manager, go to *File and Storage Services* > *iSCSI*.
  - b. From the *TASKS* dropdown list, select *New iSCSI Virtual Disk*.
  - c. The wizard prompts for access server details. The access server is the same as the iSCSI initiator. You can obtain the iSCSI initiator details by doing the following:
    - i. In Server Manager on the iSCSI initiator server, go to *Tools* > *iSCSI Initiator*.
    - ii. On the *Configuration* tab, note the *Initiator Name* value.

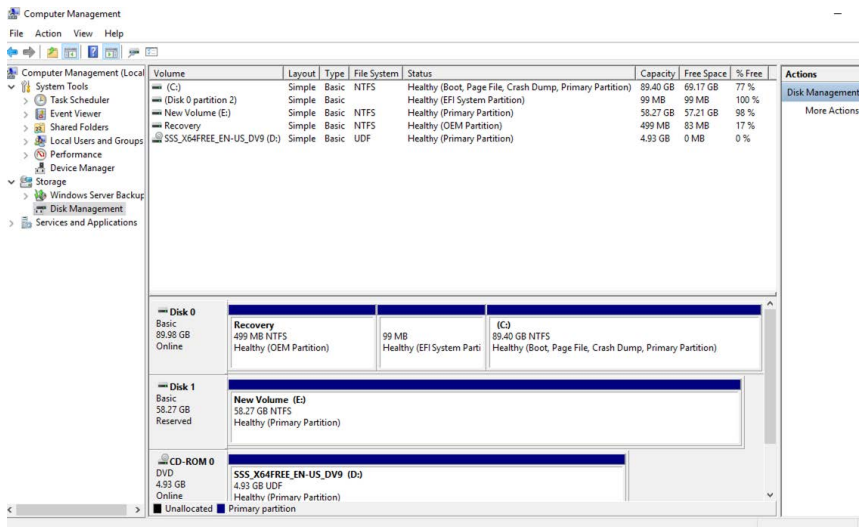


- d. Provide the value that you obtained in step 6 in the wizard.
    - e. Repeat steps 6-7 if you have multiple iSCSI initiator servers.
4. On the iSCSI initiator server, on the *Targets* tab, enter the target server name or IP address in the *Target* field.

5. Click *Quick Connect*. The discovered targets should autopopulate. Click *Connect*.



6. The *Targets* tab should show the status as connected. If not, click *Connect*.
7. After the target connects, on the *Volumes and Devices* tab, click *Auto Configure*. The volume list autopopulates with some configuration. Click *OK*. Repeat this step on other iSCSI initiator servers as needed.
8. Refresh the *File and Storage Services > File and iSCSI Services* page on the iSCSI target server. The virtual disk status displays as connected.
9. Initialize the virtual disk on the iSCSI initiator server:
- In Server Manager, go to *Tools > Computer Management > Storage > Disk Management*.
  - The new volume displays as offline. Right-click on it, then select *Online*.
  - Right-click the volume again, then select *Initialize Disk*.
  - Select the necessary partition style. In this example, *MBR* is selected.
  - At this point, the disk displays as online, but the disk space is unallocated. Right-click the disk, select *New Simple Volume*, and complete the process in the wizard.



- f. Confirm that you can see the new volume on the iSCSI initiator server. The volume should not contain any files, as the database is not installed. After installing the database, you can see Microsoft SQL files written to the virtual disk.
- g. Repeat the process on other iSCSI initiator servers as needed.

## Configuring Windows clustering

Configuring Windows clustering is required for Microsoft SQL database clustering.

### To configure Windows clustering:

1. Install the failover clustering role:
  - a. In Server Manager on the DBSRV-1 server, on the *Manage* menu, click *add Roles and Features*.
  - b. Proceed to the *Features* page. Select *Failover Clustering*. Click *Install*.
  - c. Reboot the server.
  - d. Repeat steps a-c on the DBSRV-2 server.
2. Validate the cluster configuration:
  - a. On the DBSRV-1 server, go to *Tools > Failover Cluster Manager*.
  - b. Before creating a cluster, click *Validate Configuration*.
  - c. Add the desired servers' names to the cluster list. In this example, DBSRV-1 and DBSRV-2 will be joined to a single cluster. These servers are added for validation. Click *Next*.
  - d. Select *Run all tests*. Click *Next*.
  - e. Ensure that there are no errors in the tests run and that the test report detected the virtual disk that you created in [Configuring iSCSI virtual disks on page 9](#).
3. Click *Create Cluster*.
4. Proceed through the wizard. On the *Access Point for Administering the Cluster* page, enter a name for your Windows cluster in the *Cluster Name* field. Provide a virtual IP address to tie to your Windows cluster. Click *Next* and complete the wizard to create the cluster.

Create Cluster Wizard

### Access Point for Administering the Cluster

Before You Begin  
Select Servers  
Validation Warning  
**Access Point for Administering the Cluster**  
Confirmation  
Creating New Cluster  
Summary

Type the name you want to use when administering the cluster.

Cluster Name:

The NetBIOS name is limited to 15 characters. One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.

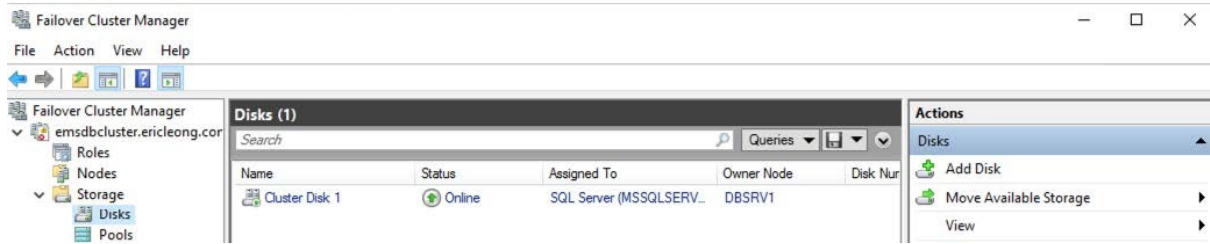
	Networks	Address
<input checked="" type="checkbox"/>	192.168.138.0/23	192.168.138.73

< Previous   Next >   Cancel

5. Go to *Storage > Disks*, and click *Add Disk*.
6. The disk that you created in [Configuring iSCSI virtual disks on page 9](#) displays. Select the disk.

7. Verify the configuration:

- a. Go to *Nodes*. Ensure that the nodes' statuses display as up.
- b. Go to *Storage > Disks*. Ensure that the disk status shows as online.



- c. On the Active Directory server, you can see that a computer account was created and that it is tied to the Windows virtual IP address.

## Configuring Microsoft SQL database clustering

### To configure Microsoft SQL database clustering:

1. Configure DBSRV-1 as the primary node:
  - a. On DBSRV-1, execute the SQL Server installer that you downloaded. The installer file downloads additional files, which you extract at a later point.
  - b. Select *New SQL Server failover cluster installation*.
  - c. An installation wizard launches. Proceed through the wizard:
    - i. On the *Instance Configuration* page, enter the computer name for the cluster in the *SQL Server Network Name* field. This is tied to the Microsoft SQL virtual IP address (VIP), which you configure later.
    - ii. In the example, *Default instance* is selected. If desired, you can select *Named instance*. Click *Next*.
    - iii. On the *Cluster Disk Selection* page, select the desired virtual disk. Click *Next*.
    - iv. On the *Cluster Network Configuration* page, configure the database VIP. Click *Next*.
    - v. On the *Server Configuration* page, configure the relevant account for services and processes to use. This example uses an Active Directory (AD) administrator account. Using a service account is recommended in a production environment. Click *Next*.

**Server Configuration**

Specify the service accounts and collation configuration.

Global Rules  
Microsoft Update  
Product Updates  
Install Setup Files  
Install Failover Cluster Rules  
Product Key  
License Terms  
Feature Selection  
Feature Rules  
Instance Configuration  
Cluster Resource Group  
Cluster Disk Selection  
Cluster Network Configuration  
**Server Configuration**  
Database Engine Configuration  
Feature Configuration Rules  
Ready to Install  
Installation Progress  
Complete

**Service Accounts** Collation

Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Agent	Administrator	*****	Manual
SQL Server Database Engine	Administrator	*****	Manual
SQL Full-text Filter Daemon Launc...	NT Service\MSSQLFDL...		Manual
SQL Server Browser	NT AUTHORITY\LOCAL...		Automatic

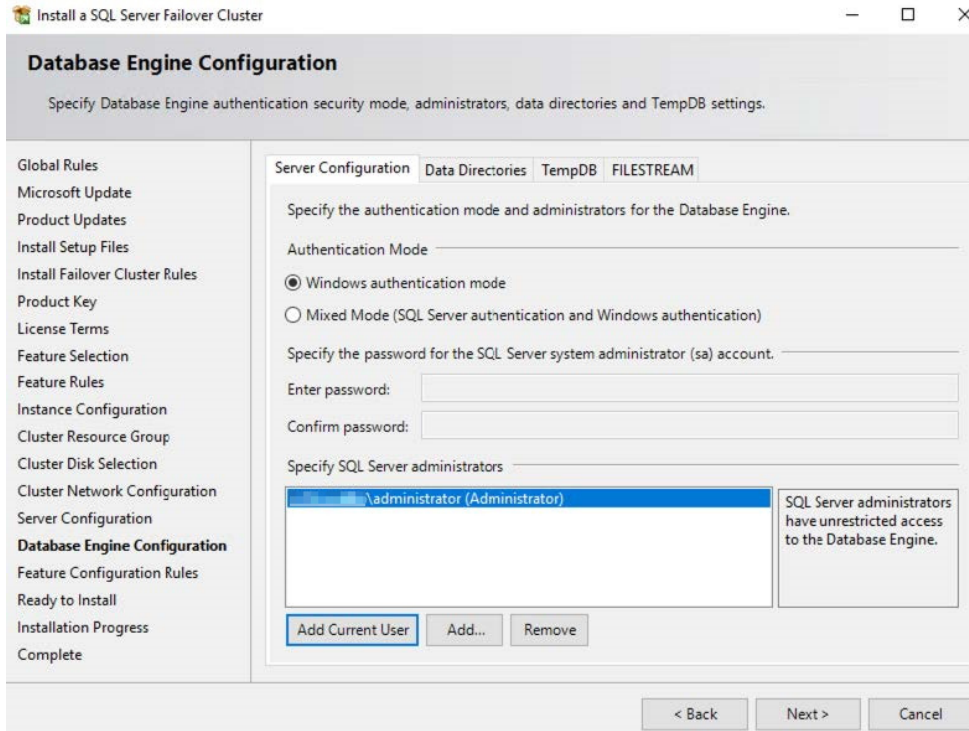
☐ Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service

This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.

[Click here for details](#)

< Back Next > Cancel

- vi. On the *Database Engine Configuration* page, configure the account to use as the database engine administrator. This example uses AD authentication mode. Click *Next*.



vii. Continue through the wizard to install SQL Server.

d. On the AD server, you can view that a computer account is created and that it is tied to the database VIP.

2. On DBSRV-2, execute the SQL Server installer that you downloaded.

3. Select *Add node to a SQL Server failover cluster*.

4. Verify the configuration:

a. On any database server, in Failover Cluster Manager, go to *Roles*. Verify that DBSRV1 is the SQL server current primary node.

b. Ensure that the database cluster status shows as running.

c. If desired, bring down DBSRV-1 to ensure that the failover happens.



## Configuring EMS HA

### To configure EMS HA:

1. Install SQL Server Management Studio (SSMS) on EMS-1 and EMS-2. This is necessary to create a SQL user later in the configuration process. It is also useful to test database connectivity prior to the installation.



2. From any server that can connect to the newly created database, log in to the database using SSMS. Use the credentials that you configured in [Configuring Microsoft SQL database clustering on page 14](#). The example also uses EMS-1 to test connectivity.
3. Create a SQL user:
  - a. In Object Explorer, right-click *Logins*, then select *New Login*.
  - b. Select SQL Server authentication.
  - c. Enter the desired password.
  - d. Deselect *Enforce password policy*.
  - e. On the *Server Roles* page, select *sysadmin*. Click *OK*.
4. In Object Server, right-click the SQL server, then select *Properties*.
5. On the *Security* page, under *Server authentication*, select *SQL Server and Windows Authentication mode*. Click *OK*.
6. Do one of the following:
  - a. In 7.0.8 and later versions, EMS does not rely on FILESTREAM for file synchronization between EMS nodes. Instead, it uses network share. If using 7.0.8 or a later version, install EMS by doing the following:
    - i. Create and share a folder on the network on a third server that is not one of the EMS servers. This file share is used to share files between EMS nodes. All EMS nodes should be able to access the file share. The folder is created on a third server to ensure that if an EMS node becomes unreachable, access to shared resources is not lost. During EMS installation, the installer automatically mounts the file share as the W:\ drive. Ensure that the W:\ drive is free on all EMS nodes. You should not use an existing drive.
    - ii. On EMS-1, open Command Prompt as an administrator.
    - iii. Run the following command:

```
FortiClientEndpointManagementServer_7.0.11.0584_x64.exe SQLServer=DBVIP
SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=1
FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator
FileStorageNicPass=Admin123! BackupDir=\\EMS-1\backup DBInitialSize=31MB
DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31
DBQueryTimeout=61
```

Parameter	Description
ScriptDB=1	Specifies that this is the primary active server.
BackupDir	Configured to \\EMS-1\backup, which is a locally shared folder on EMS-1. EMS and the SQL service user must have read/write/modify permissions to this folder.
FileStorageNic	Fileshare path.
FileStorageNicUser	Username for account with read/write/modify permissions to the shared folder.
FileStorageNicPass	Password for account with read/write/modify permissions to the shared folder.

The following is an example of the command when using a named SQL instance. In this example, the SQL instance is EMSNAMED: FortiClientEndpointManagementServer\_7.0.11.0584\_x64.exe SQLServer=DBVIP\EMSNAMED SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=1 FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator FileStorageNicPass=Admin123! BackupDir=\\EMS-1\backup DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61



- iv. On EMS-2, open Command Prompt as an administrator. Run the following command:



You must use a unique backup directory for each EMS node. The following shows BackupDir values for an example HA configuration with one primary (EMS 1) and two secondary EMS nodes (EMS 2 and 3):

- Primary (EMS 1): BackupDir=\\EMS-1\backup
- Secondary (EMS 2): BackupDir=\\EMS-2\backup
- Secondary (EMS 3): BackupDir=\\EMS-3\backup

All EMS nodes share the same FileStorageNic.

```
FortiClientEndpointManagementServer_7.0.11.0584_x64.exe SQLServer=DBVIP
SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=0
FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator
FileStorageNicPass=Admin123! BackupDir=\\EMS-2\backup DBInitialSize=31MB
DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31
DBQueryTimeout=61
```

Parameter	Description
ScriptDB=0	Indicates the upgrade does not execute scripts to upgrade the database because you upgraded the database in step c.
BackupDir	Configured to \\EMS-2\backup, which is a locally shared folder on EMS-2. EMS and the SQL service user must have read/write/modify permissions to this folder.
FileStorageNic	Fileshare path.
FileStorageNicUser	Username for account with read/write/modify permissions to the shared folder.
FileStorageNicPass	Password for account with read/write/modify permissions to the shared folder.

The following is an example of the command when using a named SQL instance. In this example, the SQL instance is EMSNAMED: FortiClientEndpointManagementServer\_7.0.11.0584\_x64.exe SQLServer=DBVIP\EMSNAMED SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=0 FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator FileStorageNicPass=Admin123! BackupDir=\\EMS-2\backup DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61

- b. If using EMS 7.0.7 or an earlier version, install EMS on the EMS-1 and EMS-2 servers by doing the following:
- i. On EMS-1, open Command Prompt as an administrator. Run the following command. ScriptDB=1 indicates that this is the primary, active server. BackupDir is configured to \\EMS-1\backup, which is a locally shared folder on EMS-1. EMS and the SQL service user must have read/write/modify permissions to this folder:

```
FortiClientEndpointManagementServer_7.0.7.0398_x64.exe SQLServer=DBVIP
SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=1
BackupDir=\\EMS-1\backup DBInitialSize=31MB DBInitialLogSize=4MB
DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61
```

The following shows an example of the command when using a named SQL instance:

```
FortiClientEndpointManagementServer_7.0.7.0398_x64.exe SQLServer=DBVIP\EMSNAMED
SQLUser=emsha SQLUserPassword=admin InstallSQL=0 ScriptDB=1 BackupDir=\\EMS-
```

```
1\backup DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB
DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61
```

- ii. On EMS-2, open Command Prompt as an administrator. Run the following command. `ScriptDB=0` indicates the upgrade will not execute scripts to upgrade the database, because the database was upgraded in step a. `BackupDir` is configured to `\\EMS-2\backup`, which is a locally shared folder on EMS-2. EMS and the SQL service user must have read/write/modify permissions to this folder:



You must use a unique backup directory for each EMS node. The following shows `BackupDir` values for an example HA configuration with one primary (EMS 1) and two secondary EMS nodes (EMS 2 and 3):

- Primary (EMS 1): `BackupDir=\\EMS-1\backup`
- Secondary (EMS 2): `BackupDir=\\EMS-2\backup`
- Secondary (EMS 3): `BackupDir=\\EMS-3\backup`

All EMS nodes share the same `FileStorageNic`.

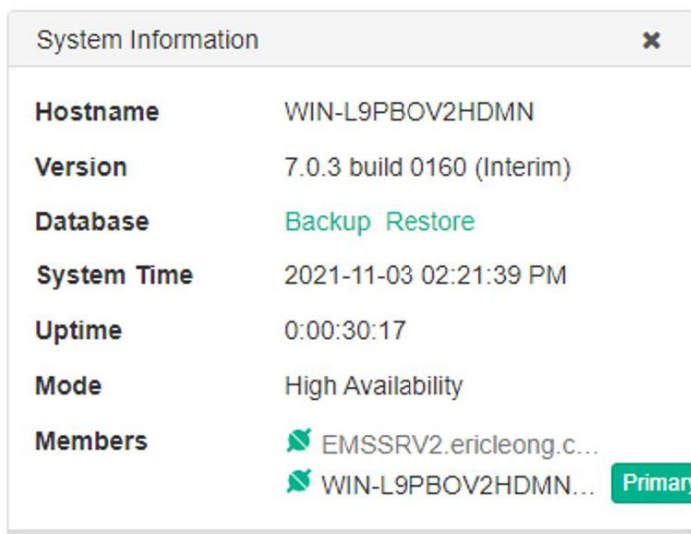
```
FortiClientEndpointManagementServer_7.0.7.0398_x64.exe SQLServer=DBVIP
SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=0
BackupDir=\\EMS-2\backup DBInitialSize=31MB DBInitialLogSize=4MB
DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=611
```

The following shows an example of the command when using a named SQL instance:

```
FortiClientEndpointManagementServer_7.0.7.0398_x64.exe SQLServer=DBVIP\EMSNAME
SQLUser=emsha SQLUserPassword=admin InstallSQL=0 ScriptDB=0 BackupDir=\\EMS-
2\backup DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB
DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61
```

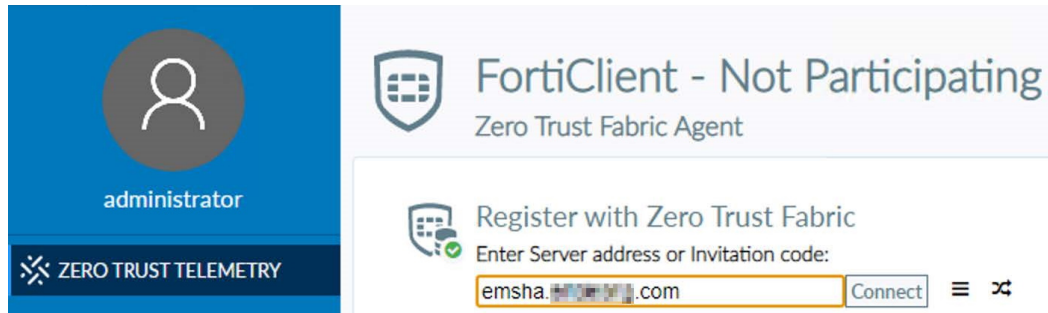
## 7. Configure EMS:

- Log in to EMS on the primary server, EMS-1.
- Go to *Dashboard > Status > License Information widget > Configure License*.
- For *License Source*, select *File Upload*.
- Click *Browse* and locate the license key file.
- Click *Upload*. The license is automatically synchronized to EMS-2. You do not need to upload two licenses.



- Go to *System Settings > EMS Settings*. Enable *Remote HTTPS access*.
- In the *FQDN* field, enter the FQDN based on the A record that you created in [Configuring AD and DNS settings on page 8](#). These settings will be synchronized to EMS-2.

8. If desired, generate installers from EMS-1 to autopopulate the EMS server address. If you have a separate installer, enter the EMS FQDN when registering FortiClient to EMS.



9. Stop EMS services on EMS-1 to test the failover.

# Upgrading EMS HA

## To upgrade EMS in HA:

1. Stop all EMS services on all secondary EMS servers. This is to avoid failover while upgrading the primary EMS server.
2. While EMS services are running on the primary server, open Command Prompt as an administrator and install the EMS version that you want to upgrade to by doing one of the following:

- To upgrade EMS to 7.0.8 or a later version, run the following command. The following example command upgrades EMS to 7.0.11:

```
FortiClientEndpointManagementServer_7.0.11.0584_x64.exe SQLServer=DBVIP SQLUser=emsha
SQLUserPassword=123456789 InstallSQL=0 ScriptDB=1
FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator
FileStorageNicPass=Admin123! BackupDir=\\EMS-1\backup DBInitialSize=31MB
DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31
DBQueryTimeout=61
```

- To upgrade EMS to 7.0.7 or an earlier version, run the following command. The following example command upgrades EMS to 7.0.7:

```
FortiClientEndpointManagementServer_7.0.7.0398_x64.exe SQLServer=DBVIP SQLUser=emsha
SQLUserPassword=123456789 InstallSQL=0 ScriptDB=1 BackupDir=\\EMS-1\backup
DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11%
DBLoginTimeout=31 DBQueryTimeout=61
```

3. After the primary server upgrade successfully completes, upgrade the secondary EMS server by opening Command Prompt as an administrator on the secondary server and installing the EMS version that you want to upgrade to by doing one of the following:

- To upgrade EMS to 7.0.8 or a later version, run the following command. The following example command upgrades EMS to 7.0.11:



You must use a unique backup directory for each EMS node. The following shows BackupDir values for an example HA configuration with one primary (EMS 1) and two secondary EMS nodes (EMS 2 and 3):

- Primary (EMS 1): BackupDir=\\EMS-1\backup
- Secondary (EMS 2): BackupDir=\\EMS-2\backup
- Secondary (EMS 3): BackupDir=\\EMS-3\backup

All EMS nodes share the same FileStorageNic.

```
FortiClientEndpointManagementServer_7.0.11.0584_x64.exe SQLServer=DBVIP SQLUser=emsha
SQLUserPassword=123456789 InstallSQL=0 ScriptDB=0
FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator
FileStorageNicPass=Admin123! BackupDir=\\EMS-2\backup DBInitialSize=31MB
DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31
DBQueryTimeout=61
```

- To upgrade EMS to 7.0.7 or an earlier version, run the following command. The following example command upgrades EMS to 7.0.7:



You must use a unique backup directory for each EMS node. The following shows `BackupDir` values for an example HA configuration with one primary (EMS 1) and two secondary EMS nodes (EMS 2 and 3):

- Primary (EMS 1): `BackupDir=\\EMS-1\backup`
- Secondary (EMS 2): `BackupDir=\\EMS-2\backup`
- Secondary (EMS 3): `BackupDir=\\EMS-3\backup`

All EMS nodes share the same `FileStorageNic`.

---

```
FortiClientEndpointManagementServer_7.0.7.0398_x64.exe SQLServer=DBVIP SQLUser=emsha
SQLUserPassword=123456789 InstallSQL=0 ScriptDB=0 BackupDir=\\EMS-2\backup
DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11%
DBLoginTimeout=31 DBQueryTimeout=611
```

For information on the install commands and parameters, see [Configuring EMS HA on page 15](#).

## Frequently asked questions

### How many EMS licenses does this configuration require?

This configuration requires one license. You upload this unit to the active EMS as [Configuring EMS HA on page 15](#) describes.

### Is there a preempt feature like in FortiOS high availability configuration?

No, there is no preempt feature. For example, if EMS-1 is the active unit and there is a service disruption in EMS-1, EMS-2 takes over as the active unit.

When EMS-1 comes back online, EMS-2 remains as the active unit until there are service disruptions. There is no fixed active unit.

### The DNS A record has round robin enabled, meaning that FortiClient sometimes connects to the passive EMS. What is the effect of this?

During initial registration, FortiClient connects to the EMS physical IP address, based on the DNS server response. There are two scenarios:

- The DNS server responds with the active EMS IP address. FortiClient connects to EMS without issue.
- The DNS server responds with the passive EMS IP address. FortiClient connects to the passive EMS, but receives a TCP reset (RST) from the server. After three TCP RSTs, FortiClient automatically switches and connects to the active EMS. Due to this behavior, FortiClient registration to EMS has a slight delay.

In the following screenshot, 192.168.138.73 is the passive EMS. You can see a RST packet reply from the passive EMS to FortiClient. After a while, FortiClient switches and connects to the active EMS.

No.	Time	Source	Destination	Protocol	Length	Info
2854	13.687570	192.168.138.36	192.168.138.73	TCP	66	64785 → 8013 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2855	13.687902	192.168.138.73	192.168.138.36	TCP	60	8013 → 64785 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2905	14.188278	192.168.138.36	192.168.138.73	TCP	66	[TCP Retransmission] 64785 → 8013 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2906	14.188468	192.168.138.73	192.168.138.36	TCP	60	8013 → 64785 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3005	14.690290	192.168.138.36	192.168.138.73	TCP	66	[TCP Retransmission] 64785 → 8013 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3006	14.690520	192.168.138.73	192.168.138.36	TCP	60	8013 → 64785 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4146	18.691440	192.168.138.36	192.168.138.72	TCP	66	64801 → 8013 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4147	18.691794	192.168.138.72	192.168.138.36	TCP	66	8013 → 64801 [SYN, ACK, ECN] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
4148	18.691998	192.168.138.36	192.168.138.72	TCP	54	64801 → 8013 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
4149	18.692628	192.168.138.36	192.168.138.72	TLsv1.3	375	Client Hello
4151	18.701034	192.168.138.72	192.168.138.36	TLsv1.3	1514	Server Hello, Change Cipher Spec, Application Data, Application Data
4152	18.701039	192.168.138.72	192.168.138.36	TLsv1.3	1187	Application Data, Application Data, Application Data
4153	18.701199	192.168.138.36	192.168.138.72	TCP	54	64801 → 8013 [ACK] Seq=322 Ack=2594 Win=2102272 Len=0
4159	18.723713	192.168.138.36	192.168.138.72	TLsv1.3	1514	Change Cipher Spec
4160	18.723713	192.168.138.36	192.168.138.72	TLsv1.3	955	Application Data, Application Data, Application Data
4161	18.724098	192.168.138.72	192.168.138.36	TCP	60	8013 → 64801 [ACK] Seq=2594 Ack=2683 Win=2102272 Len=0

FortiClient Telemetry connections behave in the same manner.

### What services run on the passive EMS server?

Only the FortiClient Endpoint Management Server Monitor Service runs on the passive EMS server.

After failover occurs and the passive EMS server changes its status to become the active EMS server, all other EMS services automatically start running.

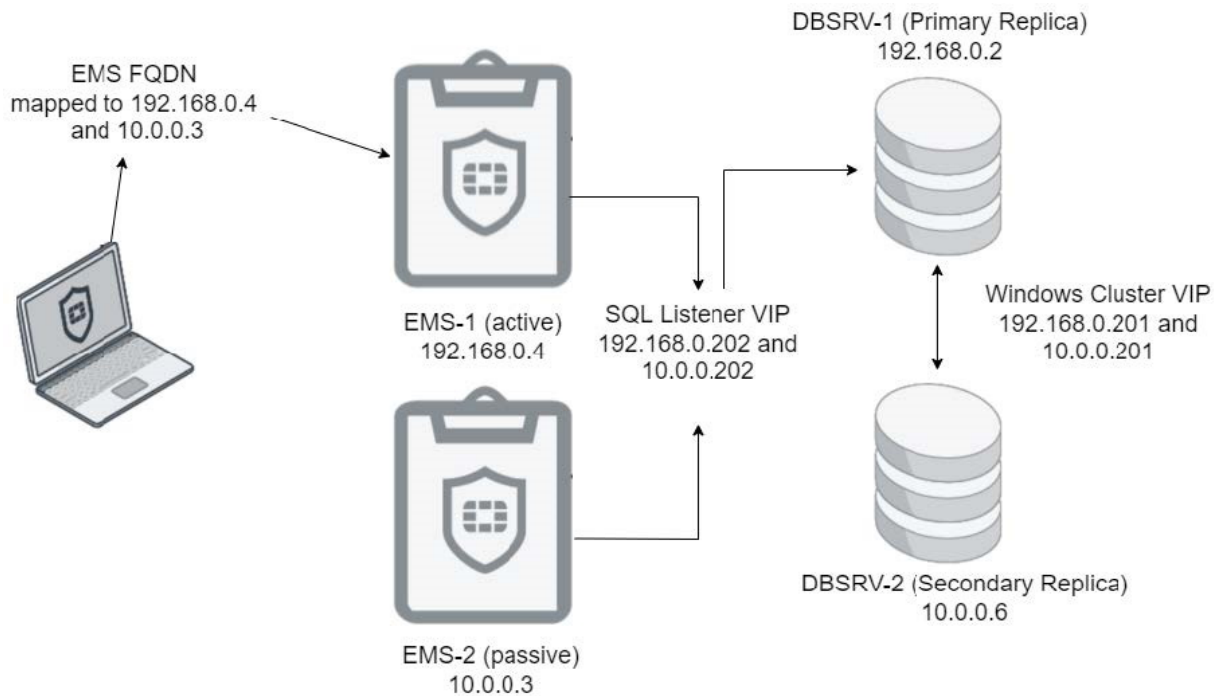
# Always on HA in multisubnet environment

This document provides information about deploying FortiClient EMS using always on high availability (HA) in a multisubnet environment. It aims to provide a step-by-step guide on EMS HA with some basic coverage of Windows clustering and always on HA groups. There may be inaccuracies as regards to Windows clustering and always on HA groups. Do not use this guide for database architecture design.

SQL Server Enterprise supports always on HA.

The example deployment that this document describes uses the following components:

- FortiClient EMS
- FortiClient
- Windows Server 2019 Standard Edition
- Microsoft SQL Server 2019 Enterprise
- Microsoft SQL Server Management Studio 18



This example uses two subnets. EMS-1 and DBSRV-1 are in subnet 192.168.0.0/24, and EMS-2 and DBSRV-2 are in subnet 10.0.0.0/16.

Note the following:

- For EMS 7.0.7 and earlier versions, for file synchronization between HA nodes, you must enable FILESTREAM on the SQL Server Database Engine instance. See [Enable and configure FILESTREAM](#).



- There are multiple ways to implement DNS and load balancing to handle EMS failover:

Method	Description
DNS round robin or failover	EMS running in HA mode must always configure a fully qualified domain name (FQDN), and FortiClient endpoints must point to a DNS server that has enabled DNS round robin or supports DNS failover, so that endpoints can always connect to the correct primary EMS server. Endpoint users must ensure that endpoints do not cache the DNS result for more than 30 seconds so that FortiClient can resolve the FQDN to the new primary EMS server with a new IP address in case EMS failover happens quickly.
Load balancer	DNS round robin configuration may cause Fortinet Security Fabric connector to send data to the failover node, which by design has all but the monitor FCEMS services off. This results in Fabric connection failure. To overcome this limitation, set up the <a href="#">Fabric connection using traffic manager</a> or <a href="#">FortiGates as a load balancer</a> .

- If logged in to an EMS server as a domain user, add the domain user to the local logon as a service. Otherwise, EMS services may not start up properly.
- All machines should have complete network reachability.

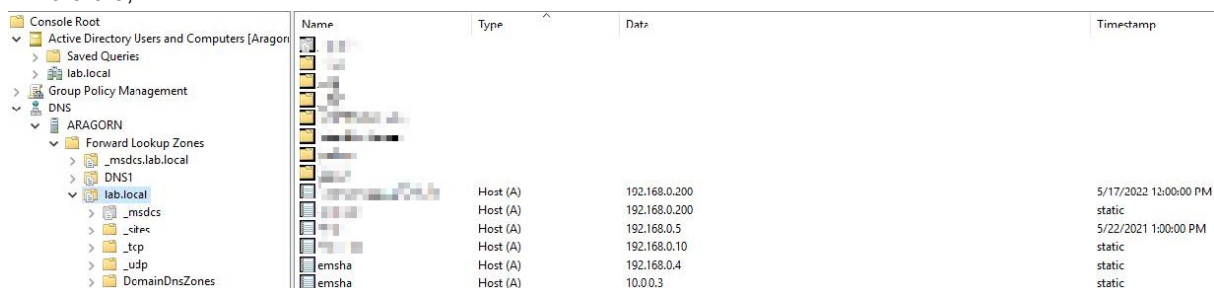
## Configuring Active Directory and DNS settings

This deployment has the following prerequisites:

- All servers and virtual machines must belong to the same domain.
- In this deployment, the Active Directory (AD) server also acts as a DNS server. The configuration requires you to configure DNS settings in AD.

### To configure AD and DNS:

- In Server Manager on the AD server, go to *Tools > DNS*.
- Right-click the DNS server, then select *Properties*.
- In the *Properties* dialog, go to the *Advanced* tab.
- Ensure that *Enable round robin* is selected. Click *OK*.
- Create two A records on the DNS server that have the same name, but point to their respective EMS servers. In this example, the records share the name "emsha". One points to 192.168.0.4, which is "EMS-Active". The other points to 10.0.0.3, which is "EMS-Passive".



The screenshot shows the Windows DNS console with the following structure in the left pane: Console Root > Active Directory Users and Computers [Aragorn] > Saved Queries > lab.local > Group Policy Management > DNS > ARAGORN > Forward Lookup Zones > \_msdcs.lab.local > DNS1 > lab.local > \_msdcs > \_tcp > \_udp > DcmainDnsZones.

Name	Type	Data	Timestamp
emsha	Host (A)	192.168.0.200	5/17/2022 12:00:00 PM
emsha	Host (A)	192.168.0.200	static
emsha	Host (A)	192.168.0.5	5/22/2021 1:00:00 PM
emsha	Host (A)	192.168.0.10	static
emsha	Host (A)	192.168.0.4	static
emsha	Host (A)	10.0.0.3	static



6. On a system joined to the AD, open Command Prompt and run `nslookup <DNS record name>.<domain>`. It should return the two IP addresses of the EMS instances that you configured in step 5.

```
C:\Users\administrator.LAB>nslookup emsha.lab.local
Server: UnKnown
Address: 192.168.0.200

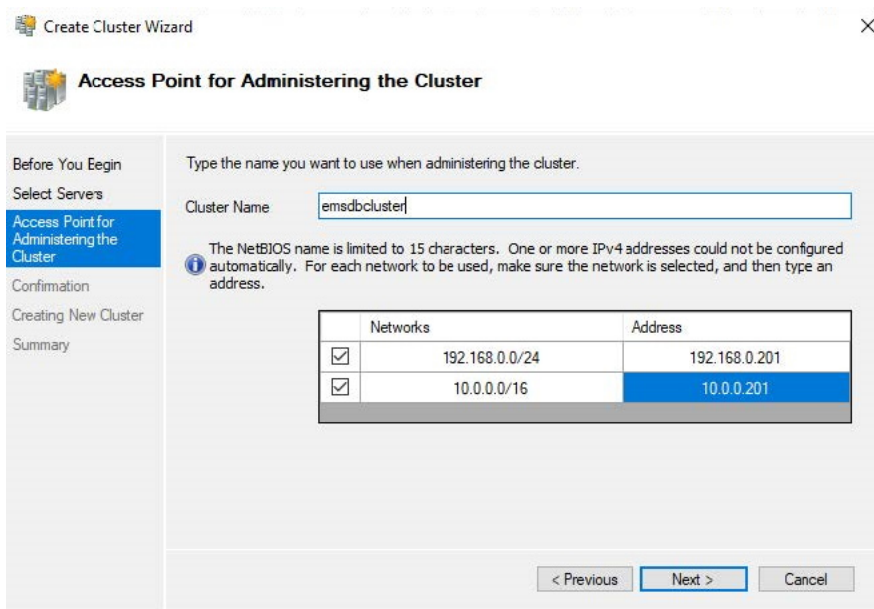
Name:     emsha.lab.local
Addresses: 10.0.0.3
          192.168.0.4
```

## Configuring Windows clustering

Configuring Windows clustering is required for Microsoft SQL always on high availability.

### To configure Windows clustering:

1. Install the failover clustering role:
  - a. In Server Manager on the DBSRV-1 server, on the *Manage* menu, click *add Roles and Features*.
  - b. Proceed to the *Features* page. Select *Failover Clustering*. Click *Install*.
  - c. Reboot the server.
  - d. Repeat steps a-c on the DBSRV-2 server.
2. Validate the cluster configuration:
  - a. On the DBSRV-1 server, go to *Tools > Failover Cluster Manager*.
  - b. Before creating a cluster, click *Validate Configuration*.
  - c. Add the desired servers' names to the cluster list. In this example, DBSRV-1 and DBSRV-2 will be joined to a single cluster. These servers are added for validation. Click *Next*.
  - d. Select *Run all tests*. Click *Next*.
  - e. Ensure that there are no errors in the tests run.
3. Click *Create Cluster*.
4. Proceed through the wizard. On the *Access Point for Administering the Cluster* page, enter a name for your Windows cluster in the *Cluster Name* field. Provide a virtual IP address to tie to your Windows cluster. Click *Next* and complete the wizard to create the cluster.



5. Verify the configuration:

- a. Go to *Nodes*. Ensure that the nodes' statuses display as up.
- b. Go to *Networks*. Ensure that the network status shows as up.
- c. Confirm that only one IP address is online at a given time.



- d. On the Active Directory server, you can see that a computer account was created and that it is tied to the Windows virtual IP address.

6. Go to *More Actions > Configure Cluster Quorum Settings* to configure the cluster quorum configuration to use a file share. A file share witness is a share that failover cluster uses as a vote in the cluster quorum:

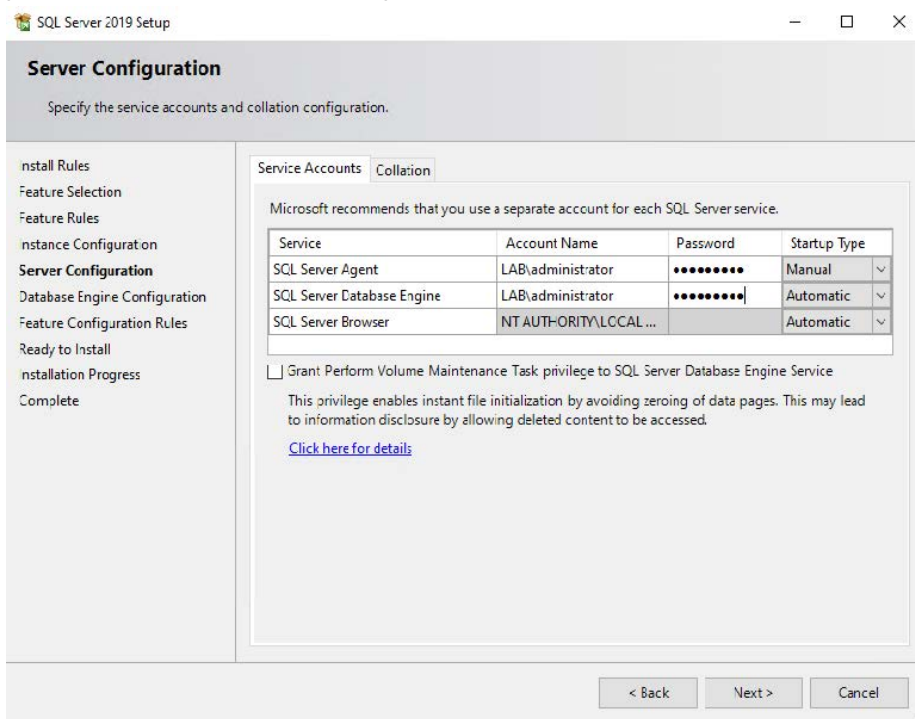
- a. For the *Quorum Configuration Option* field, select *Select the quorum witness*.
- b. As the quorum witness, select *Configure a file share witness*.
- c. Browse to the desired file share path and complete the wizard for the cluster quorum settings. Ensure that this file share is not on any cluster nodes.

## Installing SQL and enabling always on HA

### To install SQL and enable always on HA:

1. Configure an always on high availability group on DBSRV-1:
  - a. On DBSRV-1, execute the SQL Server installer that you downloaded.
  - b. Select *New SQL Server stand-alone installation* or *add features to an existing installation*.
  - c. In the example, *Default instance* is selected. If desired, you can select *Named instance*. Click *Next*.

- d. On the *Server Configuration* page, configure the relevant account for services and processes to use. This example uses an Active Directory LAB\administrator account. Using a service account with appropriate permissions is recommended in a production environment. Click *Next*.



- e. On the *Database Engine Configuration* page, configure the account to use as the database engine administrator. This example uses mixed mode. Click *Next*.
- f. Continue through the wizard and complete SQL Server installation.
- Run the SQL Server Configuration Manager and double-click the SQL Server (MSSQLSERVER) service to open the *Properties* dialog.
  - On the *Always On Availability Groups* tab, select *Enable Always On Availability Groups*. The Windows Server Failover Cluster field is autopopulated with the EMS cluster name. Click *OK*, and restart the SQL Server service.
  - If using EMS 7.0.7 or an earlier version, on the *FILESTREAM* tab, do the following:
    - Select *Enable FILESTREAM for Transact-SQL access*.
    - Select *Enable FILESTREAM for File I/O access*.
    - In the *Windows share name* field, enter MSSQLSERVER.
    - Select *Allow remote clients access to FILESTREAM data*.
  - On DBSRV-2, repeat steps 1-4 to complete the always on availability group configuration.

## Installing EMS and configuring SQL always on HA

The steps to install EMS and configure SQL always on HA differ based on the EMS version that you are using:

## Installing EMS and configuring SQL always on HA (EMS 7.0.6 or older)

### To install EMS and configure SQL always on HA:

1. Log in to DBSRV-1 using SQL Server Management Studio (SSMS), and create a SQL user:
  - a. In Object Explorer, right-click *Logins*, then select *New Login*.
  - b. Select *SQL Server authentication*.
  - c. Enter the desired password.
  - d. On the *Server Roles* page, select *sysadmin*. Click *OK*.
2. Repeat step 1 for DBSRV-2.
3. Install EMS on the EMS-1 and EMS-2 servers. For installation on both EMS servers, SQL server DBSRV-1 is used:
  - a. On EMS-1, open Command Prompt as an administrator. Run the following command. *ScriptDB=1* indicates that this is the primary, active server. *BackupDir* is configured to `\\EMS-1\share`, which is a locally shared folder on EMS-1. EMS and the SQL service user must have *read/write/modify* permissions to this folder:
 

```
FortiClientEndpointManagementServer_7.0.6.0358_x64.exe SQLServer=DBSRV-1
SQLUser=emsha SQLUserPassword= admin InstallSQL=0 ScriptDB=1 BackupDir=\\EMS-
1\share DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11%
DBLoginTimeout=31 DBQueryTimeout=61
```

The following shows an example of the command when using a named SQL instance. In this example, the SQL instance is *EMSNAME*:

```
FortiClientEndpointManagementServer_7.0.6.0358_x64.exe SQLServer=DBSRV-1\EMSNAME
SQLUser=emsha SQLUserPassword=admin InstallSQL=0 ScriptDB=1 BackupDir=\\EMS-
1\share DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11%
DBLoginTimeout=31 DBQueryTimeout=61
```
  - b. On EMS-2, open Command Prompt as an administrator. Run the following command. *ScriptDB=0* indicates the upgrade will not execute scripts to upgrade the database, because you upgraded the database in step a. *BackupDir* is configured to `\\EMS-2\share`, which is a locally shared folder on EMS-2. EMS and the SQL service user must have *read/write/modify* permissions to this folder:



You must use a unique backup directory for each EMS node. The following shows *BackupDir* values for an example HA configuration with one primary (EMS 1) and two secondary EMS nodes (EMS 2 and 3):

- Primary (EMS 1): *BackupDir*=`\\EMS-1\backup`
- Secondary (EMS 2): *BackupDir*=`\\EMS-2\backup`
- Secondary (EMS 3): *BackupDir*=`\\EMS-3\backup`

All EMS nodes share the same *FileStorageNic*.

---

```
FortiClientEndpointManagementServer_7.0.6.0358_x64.exe SQLServer=DBSRV-1
SQLUser=emsha SQLUserPassword=admin InstallSQL=0 ScriptDB=0 BackupDir=\\EMS-
2\share DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11%
DBLoginTimeout=31 DBQueryTimeout=61
```

The following shows an example of the command when using a named SQL instance. In this example, the SQL instance is *EMSNAME*:

```
FortiClientEndpointManagementServer_7.0.6.0358_x64.exe SQLServer=DBSRV-1\EMSNAME
SQLUser=emsha SQLUserPassword=admin InstallSQL=0 ScriptDB=0 BackupDir=\\EMS-
2\share DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11%
DBLoginTimeout=31 DBQueryTimeout=61
```

4. Log in to DBSRV-1 using SSMS. After installation, EMS databases *FCM* and *FCM\_Default* are created. Following are the prerequisites to add a database to an availability group. You must fulfill these prerequisites on both *FCM* and *FCM\_Default*:

- a. Right-click the database, go to *Options* and set *Recovery Model* to *Full*.
  - b. Execute the following query:  

```
ALTER MASTER KEY REGENERATE WITH ENCRYPTION BY PASSWORD = '...';
```

For example, you can enter the following:

```
ALTER MASTER KEY REGENERATE WITH ENCRYPTION BY PASSWORD = 'SQLHA123!';
```
  - c. Right-click the database, go to *Tasks*, and take a full backup.
5. Add the databases to the availability group:
- a. Right-click the *Availability Groups* folder, and select *New Availability Group Wizard*.
  - b. In the *Availability group name* field, enter the desired name.
  - c. Select *Database Level Health Detection*. Click *Next*.
  - d. On the *Select Databases* page, enter the password configured in step 5 for both databases. Click *Refresh*, then select the checkbox for each database. Click *Next*.
  - e. On the *Replicas* tab, do the following:
    - i. Click *Add Replicas*. Connect to the other SQL Server instances previously joined as nodes with the Windows Server failover cluster. In this example, it is DBSRV-2.
    - ii. Enable *Automatic Failover*.
    - iii. From the *Availability Mode* dropdown list, select *Synchronous commit*.
    - iv. For *Readable Secondary*, select *Yes*.
  - f. On the *Listener* tab, enter the following details:
    - i. In the *Listener DNS Name* field, enter the name that you will configure later in EMS configuration files.
    - ii. In the *Port* field, enter the desired port. This example uses the default SQL port, 1433.
    - iii. Add a virtual IP address for both subnets. A single subnet environment requires only one IP address. Click

Next.

**Specify Replicas**

Introduction  
Specify Options  
Select Databases  
**Specify Replicas**  
Select Data Synchronization  
Validation  
Summary  
Results

Specify an instance of SQL Server to host a secondary replica.

Replicas | Endpoints | Backup Preferences | **Listener** | Read-Only Routing

Specify your preference for an availability group listener that will provide a client connection point:

☐ Do not create an availability group listener now  
You can create the listener later using the Add Availability Group Listener dialog.

☒ Create an availability group listener  
Specify your listener preferences for this availability group.

Listener DNS Name: sqllistener

Port: 1433

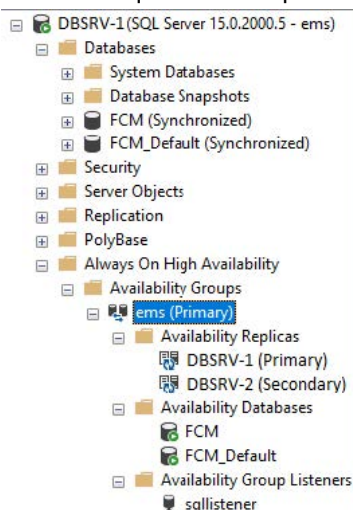
Network Mode: Static IP

Subnet	IP Address
10.0.0.0/16	10.0.0.202
192.168.0.0/24	192.168.0.202

Add... Remove

< Previous Next > Cancel

- g. On the *Select Data Synchronization* page, select *Full Database* and *Log backup*. Specify the file share path. Ensure that the file share location is not on the database servers and that the SQL user has read and write file system permissions. Click *Next*.
- h. Verify that validated checks succeed. At this point, the ems availability group has been created. FCM and FCM\_Default are added to the high availability group. You can see that the databases are synchronized. DBSRV-1 is the primary replica and DBSRV-2 is the secondary replica. On the Active Directory server, you can see that a sqllistener computer account is created and tied to provided virtual IP addresses.



6. EMS-1 and EMS-2 still point to SQL server DBSRV-1. The next step is to configure EMS servers to use the listener DNS name configured in the previous step to connect to the SQL instances. In this example, it is sqllistener:

- a. Log in to EMS-1.
- b. Go to *C:\Program Files (x86)\Fortinet\FortiClientEMS*.
- c. Open *das.conf* in a text editor, and update the *Server* field to *sqllistener*. Save the file:

```
[dbConnection]
Server = sqllistener
Port = 1433
TrustConnection = yes
Username = 0625da39429be9d12fe0e047ec6db9a47149af8186a5f898922f2942d95bc1
Password =
7dbca17d957aeec84bd3894e9388a5c1602b10c5c50524539cf63f6b591bdfa0e5c2da74
User
```

- d. Open *db.conf* in a text editor, and update the *Server* field to *sqllistener*. Save the file:

```
[Global]
ProviderString=Provider=MSOLEDBSQL
IntegratedCredentials=Trusted_Connection=yes
SQLCredentials=Uid=[ [User] ];Pwd=[ [Password] ]
SQLCredentialsGOLANG=user id=[ [User] ];password=[ [Password] ]
Server=sqllistener
Encrypt=
TrustServerCertificate=yes
User=ems
Password=Enc 785df7b54fc91b4d1fcc79bfda7f61bcc73542b60b598ac24c35f506a00d6371
BackupDir=\\GOLLUM\backup
```

- e. Stop all services on EMS-2 to avoid failover, then restart EMS services on EMS-1.
- f. Follow steps a-e for the EMS-2 server.

## Installing EMS and configuring SQL always on HA (EMS 7.0.7 or newer)

For EMS 7.0.7 or newer, you can perform the installation by directly pointing to the SQL listener instead of first installing EMS outside of the availability group and later changing the EMS configuration files to point to the SQL listener.

Creating a site automatically adds the site database to the availability group. Deleting a site automatically removes the site database from the availability group.

### To install EMS and configure SQL always on HA:

1. To create an always on high availability (HA) group, you need a database in your instance. Log in to the DBSRV-1 instance using SQL Server Management Studio (SSMS):
  - a. Create two empty databases, FCM and FCM\_Default. These are default EMS databases. Ensure that the database names are exactly as mentioned.
  - b. Right-click each database, then go to *Tasks*. Take a full backup. This is a prerequisite to add a database to an availability group.
  - c. Right-click the database. Go to options and ensure that *Recovery Mode* is set to *Full*. This is a prerequisite to add a database to an availability group.
  - d. Right-click the *Availability Groups* folder. Select the *New Availability Group Wizard* option.



- e. In the *Availability group name* field, enter the name of the availability group. Enable *Database Level Health Detection*, then click *Next*.
- f. On the *Select Databases* page, select the FCM and FCM\_Default database checkboxes to include them in the availability group, then click *Next*.
- g. On the *Replicas* tab, do the following:
  - i. Click *Add Replicas*. Connect to the other SQL Server instances previously joined as nodes with the Windows Server failover cluster. In this example, it is DBSRV-2.
  - ii. Enable *Automatic Failover*.
  - iii. From the *Availability Mode* dropdown list, select *Synchronous commit*.
  - iv. For *Readable Secondary*, select *Yes*.
- h. On the *Listener* tab, enter the following details:
  - i. In the *Listener DNS Name* field, enter the name that you will configure later in EMS configuration files.
  - ii. In the *Port* field, enter the desired port. This example uses the default SQL port, 1433.
  - iii. Add a virtual IP address for both subnets. A single subnet environment requires only one IP address. Click *Next*.

New Availability Group

**Specify Replicas**

Introduction  
Specify Options  
Select Databases  
**Specify Replicas**  
Select Data Synchronization  
Validation  
Summary  
Results

Help

**Specify an instance of SQL Server to host a secondary replica.**

Replicas | Endpoints | Backup Preferences | **Listener** | Read-Only Routing

Specify your preference for an availability group listener that will provide a client connection point:

☐ Do not create an availability group listener now  
You can create the listener later using the Add Availability Group Listener dialog.

☒ Create an availability group listener  
Specify your listener preferences for this availability group.

Listener DNS Name: sqllistener

Port: 1433

Network Mode: Static IP

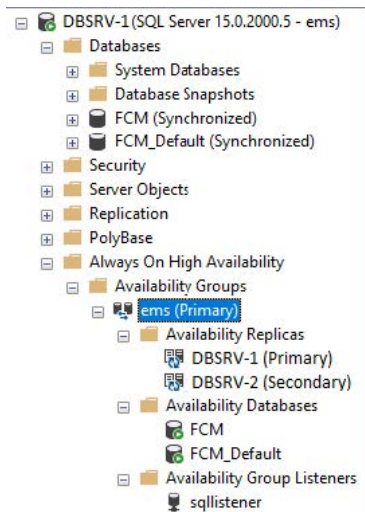
Subnet	IP Address
10.0.0.0/16	10.0.0.202
192.168.0.0/24	192.168.0.202

Add... Remove

< Previous Next > Cancel

- i. For *Data Synchronization*, select *Automatic Seeding*. Click *Next*.
- j. Verify that validated checks succeed. At this point, the ems availability group has been created. FCM and FCM\_Default are added to the high availability group. You can see that the databases are synchronized. DBSRV-1 is the primary replica and DBSRV-2 is the secondary replica. On the Active Directory server, you can see that a sqllistener computer account is created and tied to provided virtual IP addresses.





2. Install EMS on the EMS-1 and EMS-2 servers. For installation on both EMS servers, SQL server DBSRV-1 is used. Do one of the following:

- a. If using EMS 7.0.8 or a later version, do the following. EMS 7.0.8 and later versions do not rely on FILESTREAM for file synchronization between EMS nodes. Instead, it uses network share. Do the following:
  - i. Create and share a folder on the network. This file share is used to share files between EMS nodes. All EMS nodes should be able to access the file share. During EMS installation, the installer mounts the file share as the W:\ drive. Ensure that the W:\ drive is free on all EMS nodes.
  - ii. On EMS-1, open Command Prompt as an administrator.
  - iii. Run the following command:

```
FortiClientEndpointManagementServer_7.0.8.0484_x64.exe SQLServer=sqllistener
SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=1
FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator
FileStorageNicPass=Admin123! BackupDir=\\EMS-1\backup DBInitialSize=31MB
DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31
DBQueryTimeout=61
```

Parameter	Description
ScriptDB=1	Specifies that this is the primary node.
BackupDir	Configured to \\EMS-1\backup, which is a locally shared folder on EMS-1. EMS and the SQL service user must have read/write/modify permissions to this folder.
FileStorageNic	Fileshare path.
FileStorageNicUser	Username for account with read/write/modify permissions to the shared folder.
FileStorageNicPass	Password for account with read/write/modify permissions to the shared folder.

The following is an example of the command when using a named SQL instance. In this example, the SQL instance is EMSNAMED: FortiClientEndpointManagementServer\_7.0.8.0484\_x64.exe SQLServer=sqllistener\EMSNAMED SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=1 FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator FileStorageNicPass=Admin123!

```
BackupDir=\\EMS-1\backup DBInitialSize=31MB DBInitialLogSize=4MB
DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61
```

- iv. On EMS-2, open Command Prompt as an administrator. Run the following command:



You must use a unique backup directory for each EMS node. The following shows BackupDir values for an example HA configuration with one primary (EMS 1) and two secondary EMS nodes (EMS 2 and 3):

- Primary (EMS 1): BackupDir=\\EMS-1\backup
- Secondary (EMS 2): BackupDir=\\EMS-2\backup
- Secondary (EMS 3): BackupDir=\\EMS-3\backup

All EMS nodes share the same FileStorageNic.

```
FortiClientEndpointManagementServer_7.0.8.0484_x64.exe SQLServer=sqllistener
SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=0
FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator
FileStorageNicPass=Admin123! BackupDir=\\EMS-2\backup DBInitialSize=31MB
DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31
DBQueryTimeout=61
```

Parameter	Description
ScriptDB=0	Indicates that the upgrade does not execute scripts to upgrade the database because you upgraded the database in step iii.
BackupDir	Configured to \\EMS-2\backup, which is a locally shared folder on EMS-2. EMS and the SQL service user must have read/write/modify permissions to this folder.
FileStorageNic	Fileshare path.
FileStorageNicUser	Username for account with read/write/modify permissions to the shared folder.
FileStorageNicPass	Password for account with read/write/modify permissions to the shared folder.

The following is an example of the command when using a named SQL instance. In this example, the SQL instance is EMSNAMED: FortiClientEndpointManagementServer\_7.0.8.0484\_x64.exe SQLServer=sqllistener\EMSNAMED SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=0 FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator FileStorageNicPass=Admin123! BackupDir=\\EMS-2\backup DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61

- b. If using EMS 7.0.7, do the following:

- i. On EMS-1, open Command Prompt as an administrator. Run the following command. ScriptDB=1 indicates that this is the primary, active server. BackupDir is configured to \\EMS-1\backup, which is a locally shared folder on EMS-1. EMS and the SQL service user must have read/write/modify permissions to this folder:

```
FortiClientEndpointManagementServer_7.0.7.0398_x64.exe SQLServer=sqllistener
SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=1
BackupDir=\\EMS-1\backup DBInitialSize=31MB DBInitialLogSize=4MB
DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61
```

The following shows an example of the command when using a named SQL instance. In this example, the SQL instance is EMSNAMED:

```
FortiClientEndpointManagementServer_7.0.7.0398_x64.exe
  SQLServer=sqllistener\EMSNAME1 SQLUser=emsha SQLUserPassword=admin
  InstallSQL=0 ScriptDB=1 BackupDir=\\EMS-1\backup DBInitialSize=31MB
  DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31
  DBQueryTimeout=61
```

- ii. On EMS-2, open Command Prompt as an administrator. Run the following command. ScriptDB=0 indicates the upgrade will not execute scripts to upgrade the database, because you upgraded the database in step a. BackupDir is configured to \\EMS-2\backup, which is a locally shared folder on EMS-2. EMS and the SQL service user must have read/write/modify permissions to this folder:



You must use a unique backup directory for each EMS node. The following shows BackupDir values for an example HA configuration with one primary (EMS 1) and two secondary EMS nodes (EMS 2 and 3):

- Primary (EMS 1): BackupDir=\\EMS-1\backup
- Secondary (EMS 2): BackupDir=\\EMS-2\backup
- Secondary (EMS 3): BackupDir=\\EMS-3\backup

All EMS nodes share the same FileStorageNic.

```
FortiClientEndpointManagementServer_7.0.7.0398_x64.exe SQLServer=sqllistener
  SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=0
  BackupDir=\\EMS-2\backup DBInitialSize=31MB DBInitialLogSize=4MB
  DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61
```

The following shows an example of the command when using a named SQL instance. In this example, the SQL instance is EMSNAME1:

```
FortiClientEndpointManagementServer_7.0.7.0398_x64.exe
  SQLServer=sqllistener\EMSNAME1 SQLUser=emsha SQLUserPassword=admin
  InstallSQL=0 ScriptDB=0 BackupDir=\\EMS-2\backup DBInitialSize=31MB
  DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31
  DBQueryTimeout=61
```

3. Right-click the database and execute the following query. You must execute the query for both the FCM and FCM\_Default databases:

```
ALTER MASTER KEY REGENERATE WITH ENCRYPTION BY PASSWORD = '...';
```

For example, you can enter the following:

```
ALTER MASTER KEY REGENERATE WITH ENCRYPTION BY PASSWORD = 'SQLHA123!';
```

4. Execute `sp_control_dbmasterkey_password @db_name = N'db_name', @password = N'Password', @action = N'add'` for both EMS databases. This query applies the password that you created earlier to open the master key. The following give examples of this query:

```
sp_control_dbmasterkey_password @db_name = N'FCM', @password = N'SQLHA123!' , @action =
  N'add'
```

```
sp_control_dbmasterkey_password @db_name = N'FCM_Default', @password = N'SQLHA123!' ,
  @action = N'add'
```

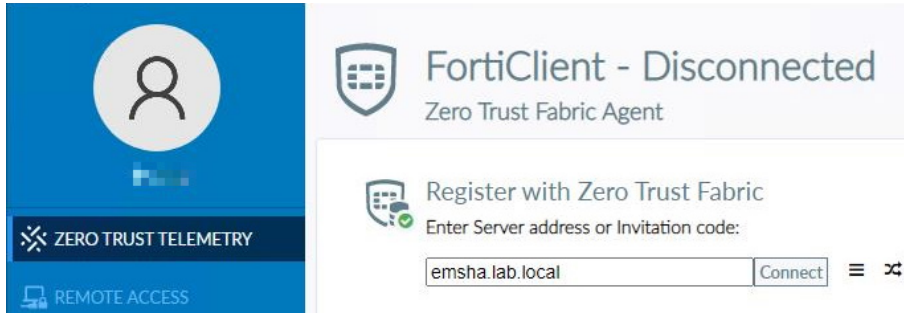
5. Log in to DBSRV-2 using SSMS. Repeat step 4 on DBSRV-2.

## Configuring EMS

### To configure EMS:

1. Configure EMS:
  - a. Log in to EMS on the primary server, EMS-1.
  - b. Go to *Dashboard > Status > License Information widget > Configure License*.

- c. For *License Source*, select *File Upload*.
  - d. Click *Browse* and locate the license key file.
  - e. Click *Upload*. The license is automatically synchronized to EMS-2. You do not need to upload two licenses.
  - f. Go to *System Settings > EMS Settings*. Enable *Remote HTTPS access*.
  - g. In the *FQDN* field, enter the FQDN based on the A record that you created in [Configuring AD and DNS settings on page 8](#). These settings will be synchronized to EMS-2.
2. Enter the EMS FQDN when registering FortiClient to EMS.



3. Stop EMS services on EMS-1 to test the failover.

## Upgrading EMS HA

### To upgrade EMS in HA:

1. Stop all EMS services on all secondary EMS servers. This is to avoid failover while upgrading the primary EMS server.
2. While EMS services are running on the primary server, open Command Prompt as an administrator and install the EMS version that you want to upgrade to by doing one of the following:
  - To upgrade EMS to 7.0.8 or a later version, run the following command. The following example command upgrades EMS to 7.0.11:
 

```
FortiClientEndpointManagementServer_7.0.8.0484_x64.exe SQLServer=sqllistener
SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=1
FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator
FileStorageNicPass=Admin123! BackupDir=\\EMS-1\backup DBInitialSize=31MB
DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31
DBQueryTimeout=61
```
  - To upgrade EMS to 7.0.7, run the following command:
 

```
FortiClientEndpointManagementServer_7.0.7.0398_x64.exe SQLServer=sqllistener
SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=1
BackupDir=\\EMS-1\backup DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB
DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61
```
  - To upgrade EMS to 7.0.6 or an earlier version, run the following command. The following example command upgrades EMS to 7.0.6:
 

```
FortiClientEndpointManagementServer_7.0.6.0358_x64.exe SQLServer=DBSRV-1
SQLUser=emsha SQLUserPassword= admin InstallSQL=0 ScriptDB=1 BackupDir=\\EMS-
1\share DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11%
DBLoginTimeout=31 DBQueryTimeout=61
```
3. After the primary server upgrade successfully completes, upgrade the secondary EMS server by opening Command Prompt as an administrator on the secondary server and installing the EMS version that you want to upgrade to by doing one of the following:

- To upgrade EMS to 7.0.8 or a later version, run the following command. The following example command upgrades EMS to 7.0.11:



You must use a unique backup directory for each EMS node. The following shows BackupDir values for an example HA configuration with one primary (EMS 1) and two secondary EMS nodes (EMS 2 and 3):

- Primary (EMS 1): BackupDir=\\EMS-1\backup
- Secondary (EMS 2): BackupDir=\\EMS-2\backup
- Secondary (EMS 3): BackupDir=\\EMS-3\backup

All EMS nodes share the same FileStorageNic.

```
FortiClientEndpointManagementServer_7.0.8.0484_x64.exe SQLServer=sqllistener
SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=0
FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator
FileStorageNicPass=Admin123! BackupDir=\\EMS-2\backup DBInitialSize=31MB
DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31
DBQueryTimeout=61
```

- To upgrade EMS to 7.0.7, run the following command:



You must use a unique backup directory for each EMS node. The following shows BackupDir values for an example HA configuration with one primary (EMS 1) and two secondary EMS nodes (EMS 2 and 3):

- Primary (EMS 1): BackupDir=\\EMS-1\backup
- Secondary (EMS 2): BackupDir=\\EMS-2\backup
- Secondary (EMS 3): BackupDir=\\EMS-3\backup

All EMS nodes share the same FileStorageNic.

```
FortiClientEndpointManagementServer_7.0.7.0398_x64.exe SQLServer=sqllistener
SQLUser=emsha SQLUserPassword=123456789 InstallSQL=0 ScriptDB=0
BackupDir=\\EMS-2\backup DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB
DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61
```

- To upgrade EMS to 7.0.6 or an earlier version, run the following command. The following example command upgrades EMS to 7.0.6:



You must use a unique backup directory for each EMS node. The following shows BackupDir values for an example HA configuration with one primary (EMS 1) and two secondary EMS nodes (EMS 2 and 3):

- Primary (EMS 1): BackupDir=\\EMS-1\backup
- Secondary (EMS 2): BackupDir=\\EMS-2\backup
- Secondary (EMS 3): BackupDir=\\EMS-3\backup

All EMS nodes share the same FileStorageNic.

```
FortiClientEndpointManagementServer_7.0.6.0358_x64.exe SQLServer=DBSRV-1
SQLUser=emsha SQLUserPassword=admin InstallSQL=0 ScriptDB=0 BackupDir=\\EMS-
2\share DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11%
DBLoginTimeout=31 DBQueryTimeout=61
```

## Managing a custom site with an availability group

### To add a custom site:

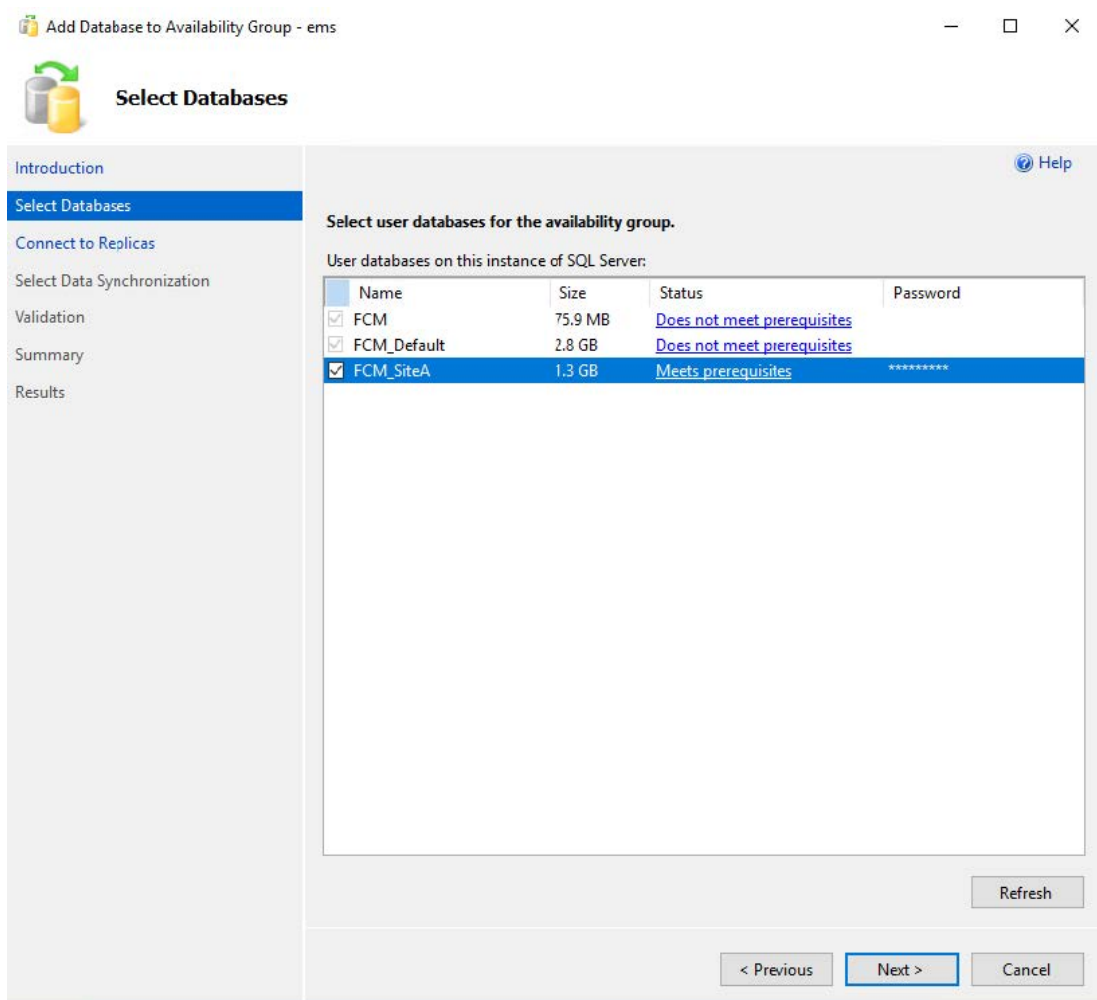
1. In EMS, enable multitenancy and create a new site as [Enabling and configuring multitenancy](#) describes.
2. Do one of the following:
  - a. For EMS 7.0.6 or an earlier version, do the following:
    - i. You can see a new database, FCM\_SiteA, on the primary SQL replica. You must manually add this database to the high availability group.



Perform the following prerequisites on the FCM\_SiteA database. These are required to add a database to the availability group:

- i. Right-click *FCM\_SiteA*. Go to *Options*, and select *Full* for *Recovery Model*.
- ii. Execute the following queries for FCM\_SiteA, using the same password that you used in [Installing EMS and configuring SQL always on HA \(EMS 7.0.6 or older\) on page 28](#).:
 

```
ALTER MASTER KEY REGENERATE WITH ENCRYPTION BY PASSWORD = '...';
```
- iii. Right-click the database. Go to *Tasks*, and take a full backup.
- ii. Under *Always On High Availability*, right-click *Availability Databases*, and select *Add Database*.
- iii. On the *Select Databases* page, select *FCM\_SiteA*, then enter the password that you created. Click *Refresh*, then select the checkbox for FCM\_SiteA.

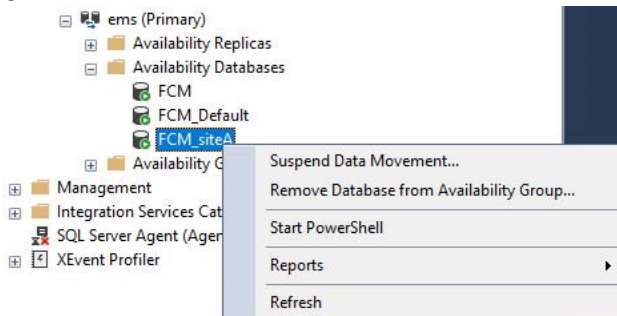


- iv. On the *Connect to Replicas* tab, connect to the other SQL Server instance previously joined as nodes with the Windows Server failover cluster. Click *Next*.
  - v. For *Data Synchronization*, select *Full Database* and *Log backup*. Enter the file share path. Click *Next*.
  - vi. Verify that the validated checks succeed. The FCM\_SiteA database is added to the availability group.
- b. For EMS 7.0.7 or a later version, do the following:
- i. When you create a new site in EMS, new custom site database, FCM\_SiteA, is added to the availability group and automatically synchronized. Log in to the primary replica.
  - ii. You must execute the following queries for the FCM\_siteA database to set and apply the password for the master key. Right-click the database and execute `ALTER MASTER KEY REGENERATE WITH ENCRYPTION BY PASSWORD = '...'`; using the password that you configured in [Installing EMS and configuring SQL always on HA \(EMS 7.0.7 or newer\) on page 31](#). The following shows the command if the password is SQLHA123!: `ALTER MASTER KEY REGENERATE WITH ENCRYPTION BY PASSWORD = 'SQLHA123!';`.
  - iii. Execute `sp_control_dbmasterkey_password @db_name = N'db_name', @password = N'Password' , @action = N'add'`. The following shows an example of this command: `sp_control_dbmasterkey_password @db_name = N'FCM_siteA', @password = N'SQLHA123!' , @action = N'add'`.
  - iv. Log in to the DBSRV-2 instance using SSMS.
  - v. Repeat step iii on DBSRV-2 to use the password created earlier to open the master key.

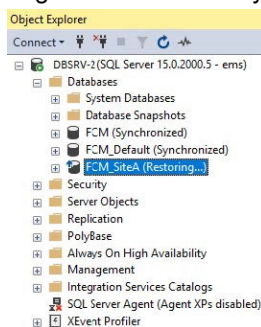


### To delete a custom site:

1. Do one of the following:
  - a. For EMS 7.0.6 or an earlier version, do the following:
    - i. Log in to the primary replica instance using SSMS.
    - ii. Go to *Availability Groups > Availability Databases*.
    - iii. Right-click the desired database, and select *Remove Database from Availability Group*.



- iv. Delete the site from EMS.
- v. Log in to the secondary replica using SSMS. FCM\_siteA is stuck in a restoring state. Delete the database.



2. For EMS 7.0.7 or a later version, do the following:
  - a. Delete the site from EMS. The site database is removed from the availability group and deleted from the primary replica.
  - b. Log in to the secondary replica using SSMS.
  - c. FCM\_siteA is stuck in a restoring state. Delete the database.

## Restoring a backup

You can restore a backup in multiple ways.

### To restore a backup while removing databases from the availability group:

1. Log in to the primary replica using SQL Server Management Studio (SSMS).
2. Go to *Availability Groups > Availability Databases*.
3. Remove the FCM and FCM\_Default databases from the availability group. If using a custom site, remove the custom site.
4. Log in to the secondary replica. The databases are stuck in the restoration state. Delete the databases.
5. Log in to the primary EMS.



6. Go to *Dashboard > Status*.
7. Click *Restore*.
8. Browse to the backup file and proceed.
9. Once EMS completes the restoration, add the EMS databases to the availability group:
  - a. Log in to the primary replica using SSMS.
  - b. Under *Always On High Availability*, right-click *Availability Databases* and select *Add Databases*.
  - c. On the *Select Database* page, enter the password that you configured in [Installing EMS and configuring SQL always on HA \(EMS 7.0.6 or older\) on page 28](#) for the EMS databases.
  - d. Select the checkboxes beside the databases. Click *Refresh*, then select the checkboxes beside the databases. Click *Next*.
  - e. On *Connect to Replicas*, connect to the other SQL Server instance previously joined as nodes with the Windows Server failover cluster. Click *Next*.
  - f. For *Data Synchronization*, select the option that you used during EMS installation and setting up the availability group.
  - g. Verify that the validated checks succeed. The databases are added to the availability group.

**To restore a backup while removing the secondary replica from the availability group:**

1. Log in to the primary replica using SQL Server Management Studio (SSMS).
2. Go to *Availability Groups > Availability Databases*.
3. Right-click the secondary replica. Select *Remove from Availability Group*.
4. Log in to the secondary replica. The databases are stuck in the restoration state. Delete the databases.
5. Log in to the primary EMS.
6. Go to *Dashboard > Status*.
7. Click *Restore*.
8. Browse to the backup file and proceed.
9. Once EMS completes the restoration, add the secondary replica to the availability group:
  - a. Log in to the primary replica using SSMS.
  - b. Under *Always On High Availability*, right-click *Availability Databases* and select *Add Replicas*.
  - c. Under *Specify Replicas*, select *Add Replica*, then *Add*. Enable *Automatic Failover*. For *Availability Mode*, select *Synchronous commit*. For *Readable Secondary*, select *Yes*. Click *Next*.
  - d. On the *Enter Passwords* tab, enter the password for the EMS databases that you configured during installation. Click *Next*.
  - e. For *Data Synchronization*, select the option that you used during EMS installation and setting up the availability group. The secondary replica is added to the availability group.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.